Opening Statement the Honorable W.J. "Billy" Tauzin
Chairman Subcommittee on Telecommunications, Trade, and Consumer Protection
Oversight Hearing on Cellular Privacy: "Is Anyone Listening? You Betcha"
February 5, 1997

This hearing is the first for the Commerce Committee or any of its Subcommittees for the 105th Congress. It's appropriate for this first hearing to remind ourselves of what we do up here. We make laws. But the measurement of our success as lawmakers only begins after we've finished making the laws. If our laws don't work as we intended, then our job isn't over. We owe it to our constituents and the American public at large to look into how our laws are working.

A few weeks back some of our leading lawmakers learned the hard way that cellular calls are not as secure as we may like. This hearing is not about that particular case. But that case raised a lot of questions for average Americans about how secure their own calls are, and why there aren't laws out there protecting them from folks who want to eavesdrop There are over 100 million wireless telephones in use in America today: 60 million cordless phones and nearly 45 million cellular and PCS phones. Every time one of these phones is used, there may be someone listening in.

There *are* laws on the books protecting the privacy of these calls. There are laws prohibiting people from buying scanners and using them to intercept wireless calls. There *are* laws prohibiting people from modiig scanners for others and advertising such modifying services. But apparently, they may not be working the way Congress intended, so it's our job to find out why. We in Congress gave responsibility to implement these laws to certain expert agencies. I've invited these government experts to give us their views on whether these laws are working and what we can effectively do to improve their enforcement.

We also need to understand from experts in the industry what are the capabilities of scanners -- how readily available are scanners that can intercept wireless calls? How easy are they to modify? Are these the only devices that can intercept wireless calls? Are digital cellular and personal communications services more secure? If so, when will these services be available nationwide? And over time, as digital technology becomes more commonly deployed and hackers de-code the encryption systems meant to protect callers' privacy, will digital services become less secure as digital scanners come down in price, and therefore more available for would-be scanners?

These technical questions have a larger policy context. The essence of a free society is freedom of speech. Open and unguarded discourse is a core freedom of a true democracy. Belief that conversations carried over telecommunications services are secure creates the necessary environment for open discourse. In contrast, the fear of eavesdropping casts a chill over discourse. If Americans feel they cannot speak freely over their wireless phones, for fear of a third party listening in, their confidence that we enjoy a free society is undermined. If we on the Subcommittee can help restore the public's confidence in the privacy of their wireless conversations, we will have helped enhance the quality of our democracy. By reminding people

there are laws on the books to prohibit invasions of their privacy, and that there are also technical solutions currently available to them, we will have performed an important public service.

Americans' privacy can be invaded through both illegal and "legal" interceptions of their telephone conversations. Legal wiretaps by law enforcement officials raise a number of questions that I hope to explore in this hearing. I hope to examine what limitations exist on law enforcement's use of wiretaps. What are the costs of enabling law enforcement to wiretap in a digital world? Are models used in a wireline world applicable to a wireless world? Are the costs borne by the telecommunications carriers' compliance with the Communications Assistance for Law Enforcement Act's (CALEA) capability and capacity requirements consistent with a reasonable balancing of the public's interest in private and low-cost services and law enforcement's interests? Will the implementation of CALEA's provisions, currently the subject of a pending rulemaking, be reasonable?

While we must accommodate law enforcement's goals, they must be balanced against the public's interest in private and secure communications. Indeed, CALEA itself requires that carriers comply with the intercept capability requirements with a minimum of interference with a subscriber's telecommunications services and in a manner that protects the privacy and security of information not authorized to be intercepted by law enforcement officials.

This hearing, and every hearing I will chair, has four goals: to educate Members; to educate the public; to identify problems; and to identify solutions. The problems with wireless privacy appear to be the technical properties of analog communications and the wide availability of easily modified scanners. There is a problem in enforcement, with the expert agency, the FCC, referring potential criminal cases to other agencies that may have less interest in enforcing the anti-intercept laws, due to other, and perhaps, more important law enforcement priorities. Perhaps a solution is to rationalize the respective enforcement roles of the FCC and Justice and the FBI. In the meantime there are technical solutions that can enhance callers' privacy currently available at reasonable prices in the marketplace. As Chairman of the Subcommittee, I want to ensure that Americans learn about these solutions.